MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

FLASH INGÉRENCE ÉCONOMIQUE DGSI #119

Avril 2026

RISQUES ASSOCIÉS À L'UTILISATION D'APPLICATIONS ET DE SOLUTIONS ÉTRANGÈRES DANS L'ENVIRONNEMENT PROFESSIONNEL

Ce « flash » évoque des actions d'ingérence économique dont des sociétés françaises sont régulièrement victimes.

Ayant vocation à illustrer la diversité des situations auxquelles les entreprises sont susceptibles d'être confrontées, il est mis à votre disposition pour vous accompagner dans la diffusion d'une culture de sécurité interne.

Il est également disponible sur le site internet : **www.dgsi.interieur.gouv.fr**

Par mesure de discrétion, le récit ne comporte aucune mention permettant d'identifier les entreprises visées.

Pour toute question relative à ce « flash » ou si vous souhaitez nous contacter, merci de vous adresser à :

securite-economique@interieur.gouv.fr

RISQUES ASSOCIÉS À L'UTILISATION D'APPLICATIONS ET DE SOLUTIONS ÉTRANGÈRES DANS L'ENVIRONNEMENT PROFESSIONNEL

Les applications et solutions étrangères sont aujourd'hui utilisées pour une très grande variété d'usages dont les entreprises, instituts de recherche et administrations publiques peuvent difficilement se passer : messageries instantanées, logiciels de visioconférences, stockage de données en ligne, outils d'intelligence artificielle ou encore logiciels de planification des ressources d'entreprise. De même, les échanges internationaux, notamment dans l'activité commerciale des entreprises, passent souvent par l'installation de logiciels ou applications qui peuvent être imposées par la partie étrangère.

Cependant, ces applications et solutions peuvent constituer des vulnérabilités, qui sont régulièrement sous-estimées par leurs utilisateurs et les entités qui y ont recours. Outre une exposition accrue au risque cyber, ces outils, souvent développés par des entreprises extra-européennes, peuvent comporter des risques juridiques, de sécurité, de confidentialité, de dépendance ou encore d'interruption de service.

L'usage non contrôlé de telles applications et solutions, notamment lorsqu'elles impliquent l'accès à des informations stratégiques, constitue un enjeu majeur de sécurité économique. Ce flash ingérence présente différents cas qui doivent inciter l'ensemble des utilisateurs à la prudence dans les informations partagées et les accès accordés.

1 LE PARTAGE DE DONNÉES SENSIBLES SUR UNE APPLICATION ÉTRANGÈRE EXPOSE UNE ENTREPRISE À DES NORMES EXTRATERRITORIALES

Un sous-traitant d'un grand groupe français évoluant dans un secteur stratégique a été retenu dans un appel d'offres de grande ampleur pour la gestion d'un projet international. Dans le cadre de la mise en œuvre de ce projet, le sous-traitant est amené à échanger de manière très régulière avec différents partenaires, en France et à l'étranger.

Or, dans le cadre de ces échanges, le sous-traitant utilise une solution étrangère pour toutes ses communications, sans hiérarchisation de la sensibilité des informations évoquées. Cette solution sauvegarde les échanges effectués et permet la génération automatique de résumés et de comptes rendus.

L'utilisation indifférenciée de cette solution constitue un risque important pour le sous-traitant, mais aussi pour le grand groupe français avec lequel il travaille, en exposant des procédés industriels. En effet, les données qui transitent par l'outil sont stockées sur des serveurs pouvant être consultés depuis l'étranger par le fournisseur et les autorités de son pays d'implantation. Ainsi, la société française est soumise au droit de ce pays, même si elle n'y a aucune activité.

2 UN LOGICIEL NÉCESSAIRE À L'EXPORTATION DE PRODUITS VERS L'ÉTRANGER EST SOURCE DE VULNÉRABILITÉS

Une entreprise française qui souhaitait exporter ses produits vers un pays étranger jugé prometteur a été contrainte d'installer sur son réseau informatique interne un logiciel ayant vocation à faciliter ses démarches administratives en lien avec le pays étranger.

L'installation du logiciel a effectivement permis d'effectuer correctement les démarches administratives obligatoires et de gagner du temps dans les procédures nécessaires à l'obtention des autorisations officielles. Toutefois, la sécurité du réseau informatique interne de l'entreprise française a signalé l'application étrangère comme suspicieuse.

L'analyse approfondie du logiciel par l'entreprise française a permis de constater qu'une seconde application avait été installée de manière dissimulée sur le réseau interne. À l'insu des utilisateurs, cette seconde application a installé plusieurs pilotes, dont certains contenaient des vulnérabilités, et maintenait un processus de veille permanent sur les activités du réseau interne, tout en ayant la capacité de programmer des tâches.

3 DES SALARIÉS SONT FORCÉS D'INSTALLER UNE APPLICATION LORS DE LEUR SÉJOUR À L'ÉTRANGER

Des salariés d'une entreprise française se rendent régulièrement dans un pays étranger, qui représente un important marché pour leur employeur, afin de rencontrer des partenaires, clients et prestataires.

À leur arrivée sur place, les salariés français ont été contraints d'installer une application étrangère sur leurs téléphones professionnels. Cette application leur a été présentée comme facilitant les échanges et leur séjour dans ce pays, notamment dans les démarches du quotidien et le paiement de services. Elle est également le mode de communication unique utilisé par leurs interlocuteurs sur place.

N'ayant d'autre choix que de recourir à cette application, tous les salariés l'ont installée sur leurs téléphones et ont rapidement remarqué que cette application était particulièrement intrusive et requérait, pour fonctionner, l'accès à l'ensemble des informations contenues dans leurs téléphones, constituant un risque fort de captation de données internes à leur entreprise.

Commentaires

Le recours à des applications et logiciels étrangers est bien souvent incontournable dans l'activité quotidienne d'une entreprise et dans son activité commerciale, notamment à l'étranger. De même, les recours à ces outils étrangers sont entrés dans le quotidien de la très grande majorité des salariés d'entreprise et chercheurs, aussi bien dans leur environnement privé que professionnel. Cette tendance s'explique notamment par le monopole que ces solutions opèrent sur certains segments et par leur facilité d'utilisation.

Toutefois, l'ensemble des utilisateurs de ces outils doivent être conscients des potentiels risques induits par leur utilisation, notamment en matière de protection des données, d'exposition à des risques juridiques et de fuite d'informations sensibles.

Lorsque des alternatives équivalentes existent, recourir à une solution nationale permet toutefois de réduire un certain nombre de risques évoqués dans ce flash ingérence.

PRÉCONISATIONS DE LA DGSI

◆ Avant d'avoir recours à une solution étrangère

- **Évaluer la réputation et la fiabilité du fournisseur de l'application étrangère avant de l'utiliser.** Faire preuve d'une vigilance toute particulière si l'entreprise qui l'a développée est une entreprise concurrente.

- **Évaluer les risques et les bénéfices de l'utilisation d'applications étrangères avant de les déployer.** Ce calcul doit également prendre en compte les coûts totaux d'utilisation de l'application étrangère, y compris les coûts de licence, de maintenance, de support et de formation.

- **Distinguer d'un côté l'usage d'une application (une messagerie, par exemple, où des données sensibles risquent de circuler) et de l'autre, l'hébergement des données de cette application.** Souvent, les offres commerciales sont liées : l'usage d'une application va de pair avec un hébergement en cloud via le même éditeur étranger. Pour les données sensibles, s'assurer que l'hébergement des données soit réalisé en France par un hébergeur français, voire directement par le client (*on premise*). Se méfier des solutions étrangères qui ne proposent pas cette distinction utilisation / hébergement.

- **Définir des niveaux de sensibilité des données de l'entreprise,** pour les catégoriser et leur appliquer des exigences de sécurité différenciées.

◆ Assurer un niveau de sécurité élevé pour chacune des applications utilisées à des fins professionnelles, en mettant en place une politique stricte d'encadrement de leur utilisation

- **Former les utilisateurs aux risques et précautions à prendre lors de l'utilisation d'applications étrangères.** Il s'agit notamment d'insister sur l'importance de limiter la transmission de données sensibles.

- **Mettre en œuvre une politique de restrictions logicielles sur les appareils dédiés à l'usage professionnel,** pour éviter l'installation de logiciels tiers ou, *a minima*, une liste blanche qui répertorie ceux autorisés.

- **Veiller à ne pas autoriser systématiquement l'accès des applications aux données de l'appareil concerné** et les limiter au strict minimum.

- **Archiver ou effacer les données obsolètes stockées sur les applications étrangères.** Bien veiller à utiliser un logiciel d'effacement sécurisé des données pour toute suppression.

PRÉCONISATIONS DE LA DGSI

◆ Privilégier les solutions françaises ou, à défaut, hébergées en France lorsqu'une solution française ne peut être choisie

- **Veiller à utiliser des applications certifiées par des organismes reconnus,** tels que l'Agence nationale de la sécurité des systèmes d'information (Anssi) ou le label « France Cybersecurity ». L'Anssi dispose d'un catalogue des produits, services, profils de protection et sites certifiés, qualifiés et agréés.

- **Sélectionner des logiciels libres qui permettent un contrôle interne de leur usage et évitent une situation de dépendance vis-à-vis d'un éditeur tiers.** Le Socle interministériel des logiciels libres (SILL) répertorie les logiciels préconisés par l'État, accessibles sur le site code.gouv.fr.

- **S'assurer qu'aucune donnée interne stratégique n'est hébergée hors du territoire national ou à défaut, européen.** Lorsque les données sont stockées dans un cloud, s'assurer qu'elles sont hébergées dans un serveur en France, y compris en cas de redondance ou de réplication des données par l'hébergeur.

- **Vérifier dans les conditions d'utilisation des applications l'usage qui est fait des données stockées.** Même lorsqu'il s'agit de solutions françaises, il est important d'avoir pleinement connaissance du devenir des données qui y sont intégrées.

◆ De façon générale

- **En cas d'évènement suspect lié à des applications étrangères, informer la DGSI.** Tout évènement suspect peut lui être communiqué sur son adresse électronique dédiée aux sujets de protection économique : securite-economique@interieur.gouv.fr.

MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité